RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: GRC-T02

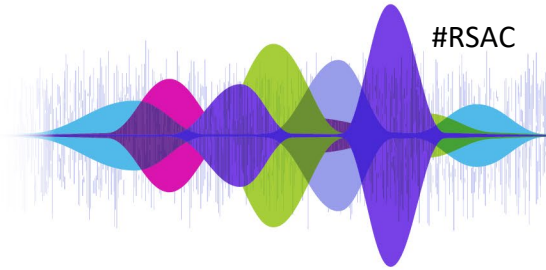
Turning Breach Fails into Best Practices

Stacy Bostjanick

Chief of Defense Industrial Base Cybersecurity
Deputy Chief Information Officer for Cybersecurity
Department of Defense
LinkedIn: https://www.linkedin.com/in/stacy-bostjanick-a3b67173

Fernando Machado

Managing Principle/CISO
Cybersec Investments
LinkedIn: https://www.linkedin.com/in/fernando-machado-cissp-cism-cca-ccp-5b5581124/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

This is Not a Drill: Why We're Here and Why It Matters.

- Every 39 seconds, another system is breached. This is no longer about 'best practices'– this is about survival.
  - MGM Grand Breach
  - Colonial Pipeline
- Cyberattacks are no longer hypothetical—they are happening as we speak
  - 75% increase in cyberattacks targeting U.S. critical infrastructure
  - 65% of breaches involved internal actors (Verizon)
  - By 2025, cybercrime is estimated to exceed $10.5 trillion USD globally
  - State-sponsored adversaries are already inside our networks
  - Check-the-box compliance efforts *will no longer suffice*

The next conflict won't start with missiles—it will start with malware.

The Alarming State of Cyber Readiness

Recent Statistics:

75% of breaches happen because of basic security failures we already know how to fix.

Organizations that use threat intelligence services identify threats 28 days faster on average (IBM)

Breakout Time for Hackers:

Less than **2 minutes** to breach. Think you're secure? Think again.

Data Breach Devastation:

The average cost of a data breach was $4.88 million in 2024, the highest average yet (IBM)

Insider Threat Explosion:

65% of data breaches in 2023 involved internal actors (Verizon).

State Sponsored Threats

The FBI has warned that Chinese hackers are "positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens.

THE ENEMY WITHIN: INSIDER THREATS

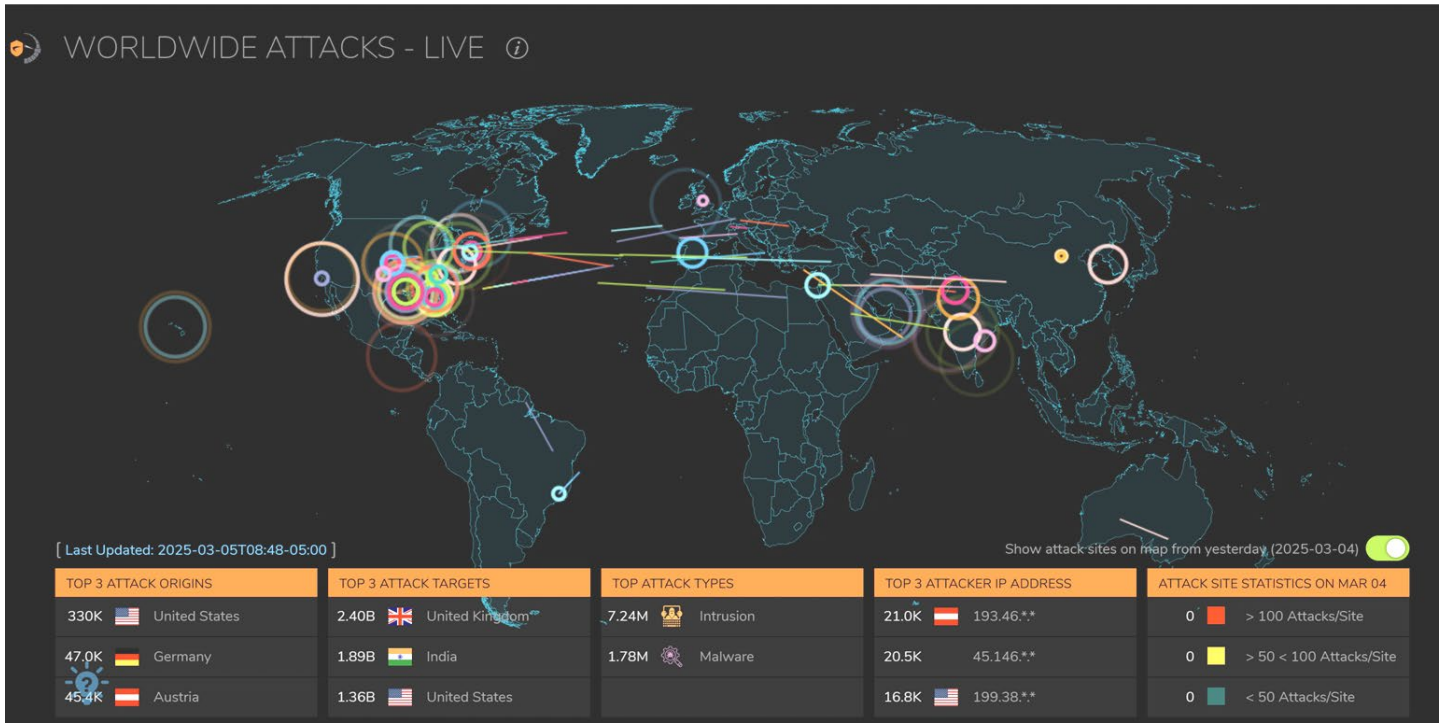
- 23 confirmed insider threat convictions involving classified data
  - This isn't theory—these are *real* convictions
- A breakdown of convictions 2022 to present:
  - Military Personnel (11 convictions)
    - Navy: 6 personnel
    - Army: 4 personnel
    - Air National Guard: 1 person
  - Defense Contractors (7 convictions)
    - Cleared personnel with access to highly classified data and systems
    - Many of these cases involved foreign influence and/or coercion
  - Government Employees (3 convictions)
    - NSA: one employee
    - CIA: two employees

Jack Teixeira (2023) – The Discord Leaks

- Who? A 21-year-old Massachusetts Air National Guard specialist
- How?
  - Had access to classified intelligence reports
  - Printed, concealed, and physically removed documents from secure environments.
  - Leaked sensitive military intelligence and national security documents on Discord
- What was exposed?
  - U.S. surveillance operations, troop deployments, and intelligence on foreign governments
    - Documents confirmed U.S. spying efforts, damaging diplomatic relations.
- The Fallout:
  - Severe national security compromise—exposed real-time military intelligence
  - DoD was forced to overhaul their insider threat monitoring policy to prevent future leaks.
- Question: What happens when insiders and nation-states work together?

From Cyber Threats to Cyber Warfare: The Escalation No One Wants to Admit

- We aren't just dealing with random breaches—nation-state actors are actively preparing for digital conflict.
- Cyber warfare isn't about stealing credit card data—it's about crippling the national infrastructure, disrupting defense operations, and weakening U.S. national security.



China's Takeover of U.S. Critical Infrastructure

- The hard truth: We didn't stop them; ***we found them too late***.
  - Volt Typhoon didn't "try" to break in—they succeeded.
  - Their implants are still out there, buried inside our critical infrastructure
  - This isn't just espionage—it's battle prep
- They're already inside. The only question is—what happens when they pull the trigger?
  - Imagine an attack synchronized with a real-world military conflict
  - Hospitals, banks, supply chains—gone.
  - Economic damage $1 trillion+
- Do we let them keep their foothold—or do we rip them out now?

The Hacker's Arsenal: Weapons Being Used Against Us Right Now

- Hacking is now plug-and-play.
  - No expertise. No barriers. Just money, time, and motive.
- You don't need an Army, you just need training (and possibly, YouTube).
  - Most of these tools are sourced from AliExpress, Temu, and other Chinese backed marketplaces.
  - YouTube provides in-depth training on the configuration and use of these devices.
- What was once military grade, is not commercial grade
- The cyber arms race isn't isolated to nation-states—it's between you and the next person with $200 and an internet connection.
- You can't ban these tools (yet) so you have to defend against them.

Concealed Devices and Insider Threats

- Water Treatment Facilities: The Perfect Cyber Weapon
  - One rogue insider. One infected USB. One catastrophic disaster.
  - Industrial Control Systems are typically wide-open targets, and attackers have proven they don't need sophisticated malware—just access.

- Real World Horror Story: Multiple Attempts to Poison U.S. Water Supplies
  - Oldsmar, Florida (2021): Attackers allegedly remotely increased sodium hydroxide (lye) levels in the city's water supply, nearly poisoning thousands.
  - San Francisco Bay Area (2021): A hacker gained access to a water treatment plant and attempted to manipulate chemical levels, putting public health at risk.
  - Iran, 2020: Reports indicate that Israeli cyber operators crippled Iran's water systems in a retaliatory strike.
- How it happens:
  - USB Drops: Rogue insiders or external attackers plant infected USBs to inject silent, destructive commands.
  - Stolen Admin Credentials: Keyloggers and phishing tactics give attackers instant control over critical systems.
  - Malware-laced Firmware Updates: Attackers embed stealthy backdoors into legitimate updates, ensuring persistent access.

A National Security Crisis

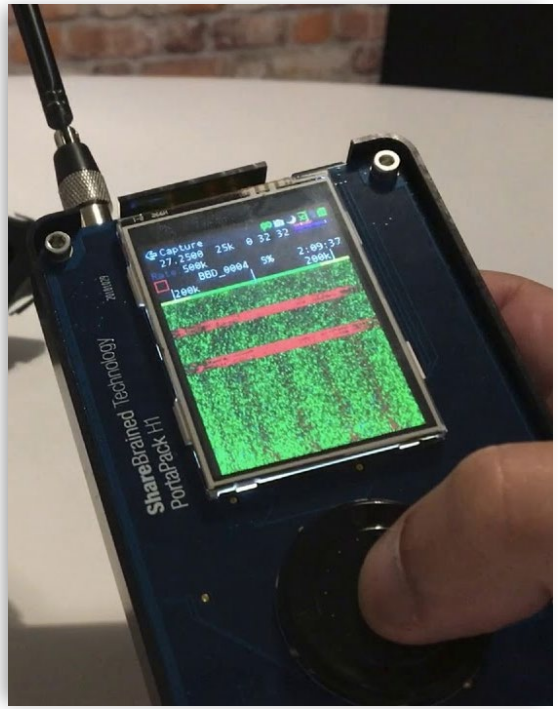
- Cyber attacks on water, power, and critical infrastructure aren't a distant threat—they are happening now.
- Emergency Services: Targeting First Responders
  - 911 Dispatch, Fire, and Law Enforcement Networks are prime cyber targets.
  - Example: A rogue employee plants a concealed keylogger, extracting and selling police dispatch credentials on the dark web—leaving our systems compromised.
- Power Grid Attacks
  - In 2023, the NSA and FBI confirmed that insiders helped plant malware inside U.S. power grids—waiting for remote activation
  - China's Volt Typhoon operation hijacked hundreds of U.S. based routers, using them to quietly establish a persistent access inside communications, energy, transportation, and water systems.
  - Intelligence agencies assess this as "pre-positioning" for catastrophic disruptions—ready to pull the trigger when geopolitical tensions escalate.
- BLUF: These attacks aren't random. They are strategic, deliberate, and designed to cripple America's critical infrastructure at the worst possible moment.
  - This isn't *cybercrime*. This is *cyber warfare.*

Concealed Devices: The Ultimate Security Bypass

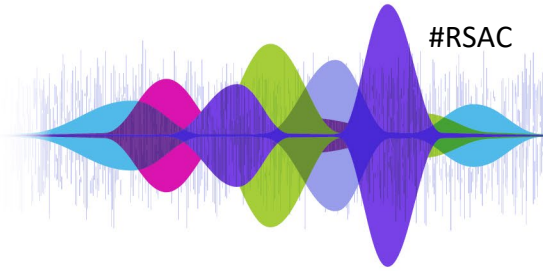
- Flipper Zero, Bash Bunny
  - Bypasses MFA, steals credentials, and deploys malware in seconds.
- USB Rubber Ducky (instant remote payload execution)
  - Looks like a normal USB drive; instead it automates system takeover.
  - Used to implant persistent malware in critical systems.
- RF Tools and Covert Wi-Fi implants (wireless hijacking)
  - If it’s got a signal, we can hack it.

The HackRF One: Can You Hack a Plane?

- **A Software Defined Radio (SDR)** used in wide-range (1MHz to 6GHz) radio frequency (RF) hacking and exploits . Provides real time signals processing, data capture and replay**.**
- Commonly used for **wireless security testing, penetration testing and research** – but in the **wrong hands, it's a powerful attack tool**
- **Why it's dangerous:** HackRF One can **jam, spoof, and manipulate** signals across aviation, GPS, IoT, and critical communications—**all in a manner that is undetectable to most security systems.**



The HackRF One: Top Exploits



- **RF Jamming: Knocking Critical Infrastructure Offline**
  - Used to disrupt/block:
    - First responder radio frequencies (fire, police, EMS)
    - Wireless networks, GPS systems, and emergency beacons
  - In 2019, attackers used RF jamming devices to disrupt emergency services in Europe.
- **GPS Spoofing: Faking Navigation to Mislead Aircraft and Drones**
  - Spoofing GPS signals can:
    - Trick autonomous vehicles, aircraft, and military drones into incorrect locations
    - Hijack supply chain logistics by falsifying GPS coordinates
- **Aviation and Shipping Communications:**
  - Aircraft-to-tower communications (potential for false ATC commands).
  - In 2023, researchers demonstrated how SDRs could be used to spoof aircraft ADS-B signals, creating fake or ghost aircraft on radar systems.

RSAC™ 2025 Conference

From Cyber Threats to Reality: Breach Failures We Need to Learn From

How Hackers Tear Through Your Defenses

- **Step 1: Gaining Entry**
  - Phishing and Social Engineering are the #1 Attack Vector.
    - Hackers don't break in; they trick you into opening the door.
      - **AT.L2-3.2.1** – *Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.*
      - **IR.L2-3.6.2 -** *Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization*
  - Compromised Credentials: Your Weakest Link.
    - Over 65% of breaches start with stolen or weak passwords.
      - **IA.L2-3.5.1** - *Identify system users, processes acting on behalf of users, and devices.*
      - **IA.L2-3.5.3 –** *Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts*
      - **AC-L2-3.1.5 -** *Employ the principle of least privilege, including for specific security functions and privileged accounts*.
  - Exploiting Unpatched Systems: The Clock is Ticking.
    - Zero-day and unpatched software give hackers free reign over your network.
      - **RA.L2-3.11.2** – *Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.*

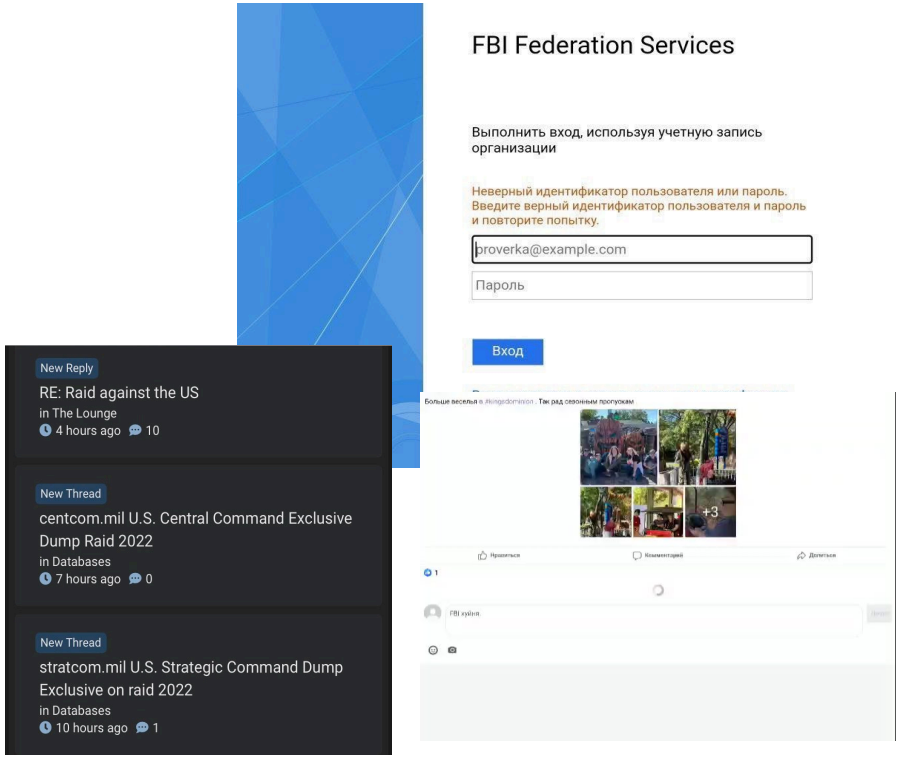
Breaches don't happen overnight—**they are a series of failures that adversaries systematically exploit.**

The Anatomy of a Breach—How Attackers Gain Control

- **Step 2: Privilege Escalation: Attackers don't break in, they level up.**
  - Weak access controls allow attackers to hijack permissions, escalating until they **own everything.**
    - **AC.L2-3.1.5 – Employ Least Privilege**
      - Ensures users have only the access necessary for their role.
    - **AC.L2-3.1.6 - Use non-privileged accounts or roles when accessing nonsecurity functions**
      - Limits exposure of privileged credentials during day-to-day activity.
    - **AC.L2-3.1.8 - Limit unsuccessful logon attempts**
      - Helps protect accounts from brute force login attempts.
  - **Admin and Service Accounts are Prime Targets:**
    - Attackers love when privileged accounts are poorly managed. Why? Because with one compromised credential they can own your environment.
  - **Case Study - Boeing 2023:**
    - Lockbit Ransomware gang hijacked credentials and moved like wildfire to exfiltrate TERABYTES of sensitive aerospace data before anyone even realized they were inside.
  - **Lesson Learned?** If you're not actively hunting…you're likely already owned.

Snatch and Dash—The Ultimate Endgame

- **Step 3: Data Exfiltration**
  - Your data is Worth Top Dollar on the Dark Web
    - Sensitive data isn't just valuable—it's a goldmine for our adversaries like China, Russia, and Iran; who want to own your environment.
    - Locking down your systems is only part of the plan. While you're scrambling to restore operations, attackers are already siphoning everything out the back door.
  - FBI Federation Services Breach:
    - Russian hackers penetrated FBI Federation Services, leveraging stolen data to access FBI Special Agents' private medical data and social media accounts.
  - Case Study: 2024 DoD Data Theft
    - A well-known DoD contractor thought they were secure—until their proprietary defense schematics showed up on the dark web.
    - Don't be tomorrow's headline ⚠️



Hackers leak documents stolen from Pentagon contractor Leidos

News

24 Jul 2024 • 3 mins

The Fallout: How a Breach Becomes a National Security Nightmare

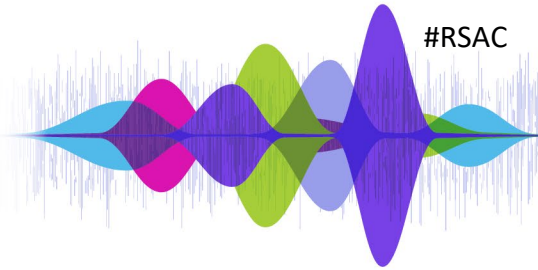
- Step 4: Operational Chaos and Strategic Impact
  - Supply Chain Impacts: A single compromised contractor can cascade failure across an entire ecosystem.
  - Attackers don't just target prime contractors—they look for the smallest, weakest link in our supply chain knowing it can cripped the whole operation.
  - Breaches in the DoD Supply Chain Result in delays in weapons systems, aircraft, and classified programs.
  - Stolen data fuels adversary R&D, directly accelerating enemy defense capabilities.
  - Every exfiltrated schematic, every leaked algorithm, is a shortcut for foreign military development.
    - The result? *Erosion of U.S. technological superiority and battlefield dominance.*

So How Do We Fix This?

From Panic to Protection: Your Action Plan for Threat Reduction

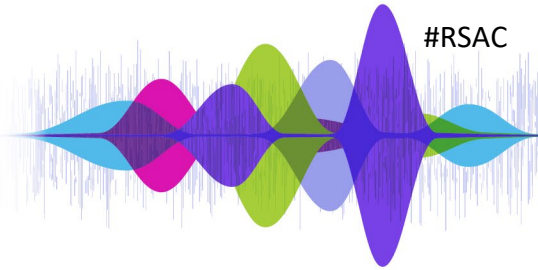
- The Harsh Reality: Your Security is NOT Ready for This
  - You don’t stop cyber warfare with compliance checklists.
  - You don’t stop insider threats by trusting your employees.
  - You don’t stop modern attacks with firewalls alone.
  - Hackers are moving faster. Your defenses need to move even faster.
- What Cybersecurity Looks Like in 2025.
  - If you’re not actively hunting threats, you’re already behind.
  - Assume breach. Authenticate everything.
  - Train like the enemy; think like the enemy. Stop them before they act.
  - No BS. No theory. Just actions that reduce the risk—right now.

Case Study: MOVEit Breach (2023)



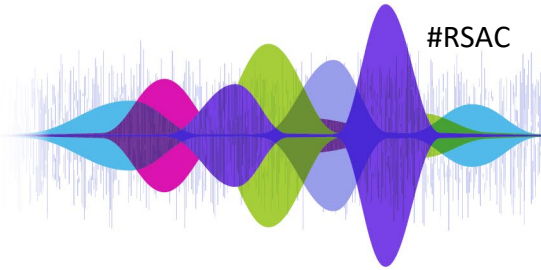
- **Breach Summary**
  - In 2023, attackers exploited a zero-day vulnerability in MOVEit, a widely used file transfer application. Multiple defense contractors and government agencies had sensitive data exfiltrated – including personnel data, contracts, and more. The breach went undetected for weeks, with data accessed from trusted third-party platforms.

Case Study: MOVEit Breach (2023)



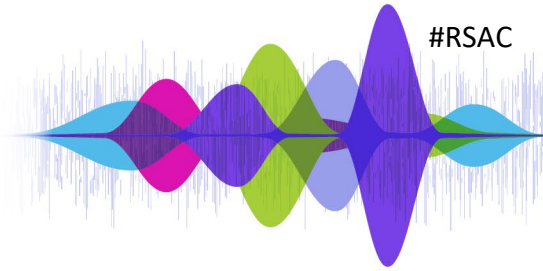
- **The Vulnerability**
  - A **zero-day SQL injection vulnerability** in MOVEit Transfer, a secure file transfer application by Progress Software, was exploited by a Russian-linked ransomware group (Cl0p)
  - This allowed attacked to gain unauthorized access to databases behind the application to exfiltrate sensitive data.
- **Scope of the Breach**
  - Thousands of organizations were impacted worldwide, including:
    - U.S. federal and state agencies
    - Defense contractors
    - Financial Institutions
    - Universities and healthcare organizations

Case Study: MOVEit Breach (2023)



- **Key Failures**
  - Many did not patch immediately after the initial vulnerability disclosure
  - Some organizations lacked real-time monitoring, allowing data exfiltration to continue undetected
  - There was an overreliance on third party tools, assuming them to be secure
  - Outbound data controls (e.g. DLP, egress filtering) were often missing or ineffective.

Case Study: CMMC Relevant Takeaways



- **SI.L2-3.14.1 –** *Identify, report, and correct system flaws in a timely manner.*
  - MOVEit's vulnerability was a zero-day, but many organizations failed to apply the patch once it became public.
    - Use a vulnerability management program that tracks vendor updates and applies emergency patches with higher urgency.
- **RA.L2-3.11.2 –** *Scan for vulnerabilities in the system and hosted applications*
  - Vulnerability scanning may have detected unpatched MOVEit instances.
    - Regular scanning could have flagged outdated instances or misconfigurations.
- **AU.L2-3.3.1 –** *Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.*
  - Logging and review of file access and transmission was clearly lacking.
    - If audit logging was properly implemented and reviewed, red flags may have been spotted earlier.

Immediate Actions: Reduce the Attack Surface

- **If they can't touch it, they likely can't hack it.**
- **Kill all unnecessary USB, WiFi, and Bluetooth ports**—treat every endpoint as a potential insider exposure.
  - Windows/macOS, Linux: Use Group Policy, MDM (Intune/Jamf), or local policies to disable USB mass storage and wireless peripherals.
  - No BYOD.
- **Segment EVERYTHING—Prevent the Single Point of Failure.**
  - Networks, applications, identities—if one breach results in access to everything, you've already lost.
  - Implement strict device approval policies—no personally owned devices in secure environments.
- **Deploy deception technology.**
  - Make attackers believe they have access while tracking their every move.
  - Deploy honeypots or fake admin credentials to lure and identify internal/external threats.

Specific Actions (Implement Within 30 Days)

- **Enforce Device Control at the OS and Endpoint Level.**
  - **Windows:** Configure **Device Guard/AppLocker** to block unauthorized executables.
  - **macOS:** Use MDM profiles to lock down USB and wireless.
  - **Linux:** Implement **udev rules** to prevent USB execution.
- **Zero Trust by Default—Assume Breach.**
  - **Isolate critical assets on separate VLANs** with strict access control policies.
  - **Apply micro-segmentation:** Prevent lateral movement using host-based firewalls (Windows Defender Firewall)
  - Remote Workforce? Deploy CASBs (Cloud Access Security Brokers) to enforce access control and visibility.

Specific Actions (Implement Within 90 Days)

- Enforce MFA on All Critical Systems—No Exceptions.
  - **Prioritize high-risk accounts first:** Admins, privileged users, remote access, and financial applications (et al.)
  - **Block SMS-Based MFA on critical assets—**use phishing resistant MFA. SMS is an open door for attackers.
- Deploy Password Manager and Strengthen Credentialing Policies
  - **Force password length over complexity** (minimum 14-16 characters, no forced resets).
  - **Block common and breached passwords** (use tools like Have I Been Pwned API for exposure checks).

Specific Actions (Implement Within 180 days)

- **Eliminate Passwords Where Possible**
  - Adopt passwordless authentication for cloud applications (Azure AD, Okta, etc.)
  - Enforce FIDO2/WebAuthn for workforce authentication—to significantly reduce phishing risk.
- **Implement Conditional Access and Risk-based Authentication**
  - Restrict access dynamically. Block logins based on device trust, location, and login behavior.
  - Implement risk-based MFA prompts (e.g., Auto deny access from high-risk countries)
- **Monitor and Detect Credential Misuse**
  - Use UEBA (User and Entity Behavior Analytics) to flag unusual credential use and patterns.
- **Lock Down Privileged Access**
  - Remove persistent admin privileges
  - Audit and rotate service account credentials.

Specific Actions (Implement Within 180 days)

- **Restrict Executable Code and Powershell.**
  - Block unauthorized scripts via AppLocker, software restriction policies, or PowerShell constrained language mode.
  - Monitor script execution logs (Sysmon for Windows, auditd for Linux)
- **Asset Management and Visibility.**
  - Deploy an asset discovery tool like Rumble, Lansweeper, or Active Directory-based tracking.
  - Automate inventory updates with SIEM integrations.
  - Remember, you can’t secure what you can’t see.

RSAC™ 2025 Conference

Many Voices.
One Community.

For more information:
fernando.machado@cybersecinvestments.us